



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,297	07/22/2003	James W. O'Toole JR.	CIS03-08(6535)	7810

47654 7590 07/24/2007

DAVID E. HUANG, ESQ.
BAINWOOD HUANG & ASSOCIATES LLC
2 CONNECTOR ROAD
SUITE 2A
WESTBOROUGH, MA 01581

EXAMINER

ALMEIDA, DEVIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

07/24/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/624,297	Applicant(s) O'TOOLE ET AL.	
	Examiner Devin Almeida	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 May 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-38 ~~16, 17, 31, 37 and 38~~ is/are pending in the application.
 4a) Of the above claim(s) 1-15, 18-30 and 33-36 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 16, 17, 31, 32, 37 and 38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☒ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This action is in response to the papers filed 5/16/2007. In response to the restriction requirement applicants elect without traverse claims 16-17, 31-32 and 37-38.

68y
Claims 1-15, 18-30 and 33-36 are withdrawn for consideration.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 16, 31, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. 2003/0226023) in view of Kielland et al (U.S. Patent # 6,081,206). Peters teaches with respect to claim 16, a method for generating an output signal from a video data acquisition system, the method comprising: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file); encrypting the first key using a second key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption); including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage); Peters does not teach implementing

a recognition algorithm to identify objects associated with the sensed images; and in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal. Kielland teaches means for identifying objects (see Kielland column 6 line 64 – column 7 line 11 i.e. License plate) associated with the sensed images (see Kielland column 6 line 64 – column 7 line 11 i.e. digital camera captures a raster image of each vehicle) and embedding encrypted data information identifying the recognized object in the output signal (see Kielland column 6 line 64 – column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have attached the unique digital identifier for the vehicle to help determine where and when the vehicle was spotted. Therefore one would be motivated to have included object data in the output signal (see Kielland column 6 line 64 – column 7 line 11).

With respect to claim 31, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images (see Peters paragraph 0004); a memory device to store at least first and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)); a processor that encrypts the video signal using the first encryption key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file), the processor

Art Unit: 2132

encrypting the first encryption key with the second encryption key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption), the processor producing an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach a recognition system to identify objects associated with the sensed images, the processor embedding encrypted data information identifying the recognized object in the output signal. Kielland teaches means for identifying objects (see Kielland column 6 line 64 – column 7 line 11 i.e. License plate) associated with the sensed images (see Kielland column 6 line 64 – column 7 line 11 i.e. digital camera captures a raster image of each vehicle) and embedding encrypted data information identifying the recognized object in the output signal (see Kielland column 6 line 64 – column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have attached the unique digital identifier for the vehicle to help determine where and when the vehicle was spotted. Therefore one would be motivated to have included object data in the output signal (see Kielland column 6 line 64 – column 7 line 11).

With respect to claim 37, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed

images (see Peters paragraph 0004); a memory device to store at least first and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)); means for encrypting the video signal using the first encryption key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file) and means for encrypting the first encryption key with the second encryption key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption) to produce an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal. Kielland teaches means for identifying objects (see Kielland column 6 line 64 – column 7 line 11 i.e. License plate) associated with the sensed images (see Kielland column 6 line 64 – column 7 line 11 i.e. digital camera captures a raster image of each vehicle) and embedding encrypted data information identifying the recognized object in the output signal (see Kielland column 6 line 64 –

Art Unit: 2132

column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have attached the unique digital identifier for the vehicle to help determine where and when the vehicle was spotted. Therefore one would be motivated to have included object data in the output signal (see Kielland column 6 line 64 – column 7 line 11).

With respect to claim 38, a computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, cause the processing device to perform the steps of: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file); encrypting the first key using a second key, the first and second key being different than each other (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption); including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach identify objects associated with the sensed images, and embedding encrypted data information identifying the recognized object in the output signal Kielland teaches means for

identifying objects (see Kielland column 6 line 64 – column 7 line 11 i.e. License plate) associated with the sensed images (see Kielland column 6 line 64 – column 7 line 11 i.e. digital camera captures a raster image of each vehicle) and embedding encrypted data information identifying the recognized object in the output signal (see Kielland column 6 line 64 – column 7 line 11). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have attached the unique digital identifier for the vehicle to help determine where and when the vehicle was spotted. Therefore one would be motivated to have included object data in the output signal (see Kielland column 6 line 64 – column 7 line 11).

Claims 16, 31, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. 2003/0226023) in view of Chainer et al (U.S. Patent # 6,397,334). Peters teaches with respect to claim 16, a method for generating an output signal from a video data acquisition system, the method comprising: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file); encrypting the first key using a second key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption); including at least the encrypted first key and encrypted video signal in the output signal (see Peters

Art Unit: 2132

paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage); Peters does not teach implementing a recognition algorithm to identify objects associated with the sensed images; and in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal. Chainer teaches means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental configuration and other characteristic and transmit then in encrypted form to help the receiver authenticate what he is looking at. One would be motivated to have sent sensor data encrypted to help the receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

With respect to claim 31, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images (see Peters paragraph 0004); a memory device to store at least first and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)); a processor that encrypts the video signal using the first encryption key (see Peters figure 1 and

paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file), the processor encrypting the first encryption key with the second encryption key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption), the processor producing an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach a recognition system to identify objects associated with the sensed images, the processor embedding encrypted data information identifying the recognized object in the output signal. Chainer teaches means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental configuration and other characteristic and transmit then in encrypted form to help the receiver authenticate what he is looking at. One would be motivated to have sent sensor data encrypted to help the receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

With respect to claim 37, an apparatus to support surveillance, the apparatus comprising: a camera to generate a video signal that varies depending on sensed images (see Peters paragraph 0004); a memory device to store at least first and second encryption keys (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)); means for encrypting the video signal using the first encryption key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file) and means for encrypting the first encryption key with the second encryption key (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption) to produce an output signal including at least the encrypted video signal and the encrypted first encryption key (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal. Chainer teaches means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3,

Art Unit: 2132

column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental configuration and other characteristic and transmit then in encrypted form to help the receiver authenticate what he is looking at. One would be motivated to have sent sensor data encrypted to help the receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

With respect to claim 38, a computer program product including a computer-readable medium having instructions stored thereon for processing data information, such that the instructions, when carried out by a processing device, cause the processing device to perform the steps of: receiving a video signal that varies depending on sensed images (see Peters paragraph 0004); encrypting the video signal using a first key (see Peters figure 1 and paragraph 0031 i.e. then encrypts some part of that captured input with a symmetric key which has been generated or provided for use with this image file); encrypting the first key using a second key, the first and second key being different than each other (see Peters figure 1 and paragraph 0031 i.e. The symmetric key is then encrypted (Block 120), preferably using public key encryption); including at least the encrypted first key and encrypted video signal in the output signal (see Peters paragraph 0032 i.e. Having encrypted both the image and the symmetric key, the image is then stored on some form of persistent storage and 0032 i.e. The encrypted symmetric key is preferably stored with the encrypted image, but alternatively may be separately stored (e.g., in a separate file)). Peters does not teach identify

Art Unit: 2132

objects associated with the sensed images, and embedding encrypted data information identifying the recognized object in the output signal. Chainer teaches means for identifying objects associated with the sensed images and embedding encrypted data information identifying the recognized object in the output signal (see Chainer figure 2 and 3, column 4 line 30 – column 6 line 17 and column 7 lines 52-61). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have recognized object based on RFID tags, iris/retinal shape, dental configuration and other characteristic and transmit then in encrypted form to help the receiver authenticate what he is looking at. One would be motivated to have sent sensor data encrypted to help the receiver authenticate what he is looking at (see Chainer column 1 lines 27-51).

Claims 17 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. 2003/0226023) in view of Kielland et al (U.S. Patent # 6,081,206) further in view of Grube et al (U.S. Patent # 5,517,568). Peters and Kielland teaches everything with respect to claim 16 above but with respect to claim 17 they do not teach randomly generating a new encryption key for encrypting different portions of the video signal over time. Grube teaches randomly generating a new encryption key for encrypting different portions of the video signal over time (see Grube column 1 line 51-67). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase

the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase security (see Grube column 1 line 51-67).

With respect to claim 32, further comprising: an encryption key generator that randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time (see Grube column 1 line 51-67).

Claims 17 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peters (U.S. 2003/0226023) in view of Chainer et al (U.S. Patent # 6,397,334) further in view of Grube et al (U.S. Patent # 5,517,568). Peters and Chainer teaches everything with respect to claim 16 above but with respect to claim 17 they does not teach randomly generating a new encryption key for encrypting different portions of the video signal over time. Grube teaches randomly generating a new encryption key for encrypting different portions of the video signal over time (see Grube column 1 line 51-67). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to generating a new encryption key for encrypting different portions of the video signal over time to increase the security of the transfer by changing the encryption thought out the transfer. One would be motivated to have randomly generating a new encryption key for encrypting different portions of the video signal over time to further increase security (see Grube column 1 line 51-67).

With respect to claim 32, further comprising: an encryption key generator that randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time (see Grube column 1 line 51-67).

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
7/5/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100